ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

An Enhancement on Request Rate-Time-Bandwidth for Limiting Replay Attack in MANET

Sreeja Nair M.P

Faculty in Computer Science & Engg., Cochin University College of Engg, Pulincunnoo,Alappuzha,Kerala, India.

Abstract: A Mobile Adhoc Network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Though each node in MANET will act as host as well as router, the security is a major issue and the chances of having the vulnerabilities and attacks are also more. Different types of attacker attempts different approaches to decrease the network performance, throughput. In this paper,I propose an enhancement of Request-bandwidth-time based on selective verification for limiting the impact of a replay attack.

Keywords*:* MANET,Replay attack,bandwidth,DoS attack.

I.INTRODUCTION

A MANET(Mobile Adhoc Network) is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission[1][2].

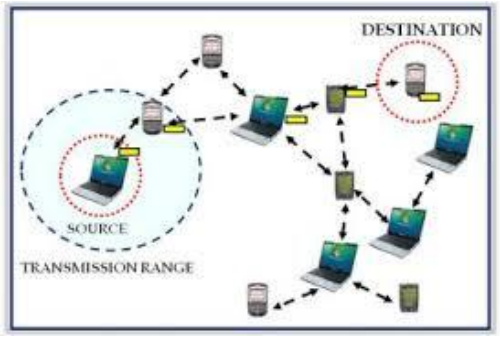


Fig 1.Mobile Adhoc Network

In a MANET, two given MNs can communicate directly when each one is in the transmission communication range of the other one. Otherwise, those MNs communicate through intermediate MNs that relay their messages. So, the success of a given communication between the sender and receiver MNs is strongly dependent on the cooperation of the intermediate MNs[2].

The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network[1]. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment. As the transmission takes place in open medium makes the MANETs more vulnerable to security attacks. In the presence of security protocol, various attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes.Securing wireless adhoc networks is a highly challenging issue.

Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central coordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network, there are a number of attacks that affect MANET. These attacks can be classified into two types[1]:

1. External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.
2. Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyse traffic between other nodes and may participate in other network activities.

Denial-of-Service (DoS) attacks in MANET can seriously affect the network connectivity and disrupt further networking functions, such as control and data message delivery[2]. In other words, we can say that DoS attacks are capable to harshly degrade the overall MANET performance. Indeed, at the physical layer, the attacker can launch a DoS attack with a wireless Jammer by sending a high power signal to cause an extremely low signal-to-interference ratio at a legitimate receiver MN. At the 802.11 MAC layer , a replay attack can be done by intercepting a valid signed messages of MN (the validation is assured by the timestamp concept) and by retransmitting them later in order to produce a DoS attack. At the network layer, a DoS attacker makes the use of the existing protocols vulnerabilities, that can be classified further into three types: routing disruption, forwarding disruption and resource consumption attacks[2]. At the application layer, a random DoS attack is to flood a network with a large number of service requests. Since the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

MNs have a limited transmission range, they expect that their neighbours relay messages to remote receiving MNs. The relayed messages are supposed to be performed by intermediate MNs with a good cooperation as a fundamental assumption of MANETs. This assumption becomes invalid when MNs have tangential or contradicting objectives. To overcome their security problems, MANETs adopt new secure solutions . When the most known attacks can be avoided, replay attacks are still subject of various research works due to their easy technique based on recording and resending a valid signed messages in the network[2].

In a DoS attack, there are no inherent limitations in the number of machines that can be used to create the attack. A DoS attack uses the distributed behaviour of the internet, with hosts owned by disparate entities around the world. These computers are then used to wage a coordinated mass-scale attack against a particular system or site. In addition, since these attacks are coming from a wide range of IP addresses, it is more difficult to block and detect at the firewall level.The DoS attack aims to disrupt some authorized activity, such as browsing web pages, or transferring money from bank account etc.This denial-of-service effect is achieved by sending messages to the destination that interfere with its operation, and make it hang, crash, reboot, or do unwanted work[4].

The DoS attack is quickly becoming more and more composite. There is variety of known attacks which creates the impression that the problem space is immense, and hard to explore and tackle. The existing systems employ various techniques to take over the problem, and it is difficult to understand their similarities and differences and to evaluate their effectiveness, performance and cost**.**

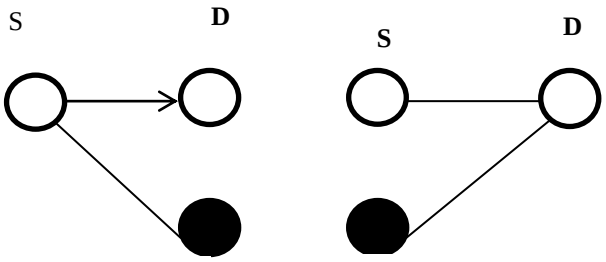
A.IEEE 802.11

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. Wireless LANs are provide 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The 802.11 MAC protocols support two models of operation called Distributed Coordination Function (DCF) and Point Coordination Function (PCF). Whereas DCF does not use a centralized control, PCF needs an access point (AP) to coordinate the activity of nodes in its area and to operate only in infrastructure-based networks. When PCF is an optional feature at different 802.11 im- plementations, DCF is obligatory[2][10].

II.RELATED WORK

What is Replay Attack?: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.[1][2][3].

1.Listening step 2.Resending step



Replay attack **Replay attack**

DoS attack is replay attack where the malicious MN can perform attack by recording old valid messages and by resending them. This makes other MNs update their internal data structure with stale information (for example updating routing table with a wrong route). The replay attack is achieved when control messages bear a digest or a digital signature without including a timestamp. Indeed, while existing mechanisms provide the guarantee to the receiving MN that the message was received as sent, there is no absolute guarantee that a message is being used as intended. The originated MN and the sent message are authenticated, but nothing else. A message that has been captured or intercepted by a malicious MN and is replayed later[2].

The replay attack is an easy DoS attack which can be produced by a malicious MN through two basic operations. The first operation is the record of listened valid messages. The second is the resend of the recorded valid messages. Indeed, for a given communication between two MNs in the network, the replay attacker intercepts messages sent to destination MN and resends them later within a valid timestamp discrepancy, independently, to any encryption mechanisms used by the sender MN. So the standard timestamp concept is not enough to limit impact of this type of DoS attacks on network performance Δt. The Figure 2 illustrates a typical replay attack scenario where malicious MN, in the first step, intercepts and records signed messages listened from sender MNs. In second step and after a waiting time, within the timestamp discrepancy interval Δt , the attacker MN resends the stored signed messages, towards the receive MN D. As a result, all resend messages by the replay attacker that verify the timestamp discrepancy present an overhead of messages which impact directly the network performance. Recent works are still using, in the process of message signature, a prefixed timestamp discrepancy Δt negotiated in the step of encryption key exchange. This choice of static timestamp gives a greatest weakness due to its independence on MN characteristics and duration of communication[1][2].

III.BACKGROUND

In existing system they presented an enhanced timestamp discrepancy aiming to limit the impact of duplicated valid messages injected by a replay attacker between a pair of communicated MNs. Their approach has the advantage that not to require any additional functions because it only based on the existing parameters defined in

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

the MAC layer of the IEEE 802.11 standard. This timestamp approach estimates approximately the date when the signed message is received and processed by a destination MN. Moreover, this estimation is a lightweight calculation and it is based on the standard parameters of 802.11 MAC layer. The sender MN begins communication after receiving the message sent by the receiver MN. In the same time, the neighbours MNs update their NAV parameter to defer access (DA) to the communication medium to avoid col lisions. So, a sent signed message from a sender MN should arrive, to the receiver MN, and be processed before the NAV time expiration. The NAV expiration is delimited by the two messages: RTS (sent by the sender MN) and CTS (sent by the receiver MN). This means that the maximum time for a signed message to reach destination is the total time including NAV time plus processing times at the sender and receiver MNs[2].

Based on this observation, we can define the enhanced timestamp discrepancy between two given communicat ing MNs, S and D as follow[2]:

$$\Delta t_{dynamic}(S,D)=T_s+NAV(CTS)+T_D$$

where:

- T_S is the time to process message at MN S.
- T_D is the time to process message at MN D.
- NAV is the time duration of communication between sender (S) and receiver (D) MNs.

IV.DRAWBACKS OF EXISTING SYSTEM

- There is a high probability attack in the shared channel since the legitimate clients and attackers share the same channel.
- Clients are allowed to send requests repeatedly to server till an acknowledgment is received. So they send repeated requests and are not concerned if there is an attack or not. They are not able to dynamically adapt to attack. Thus there is an increased bandwidth usage. So Server overhead increases due to flooding of request packets.
- Client assume that the attackers send requests a certain rate and clients always try to send requests at a rate more than the attacker rate. So knowledge of attack rates is a prerequirment.
- Server does not perform any node verification.
- Client is not aware whether there is attacker in the network or not.

V.PROPOSED SYSTEM

In this paper I introduced an enhancement on Request Rate, Bandwidth, Time based on selective verification protocol for limiting Replay attack[4].

A.Setting

The first step of the protocol is a REQ packet from a client C to the server S. In response, the server sends back an ACK to the client. Each client employs a timeout window of duration T determined by the worst-case expected round-trip delay between the clients and the server: If after transmission of an REQ, a client does not receive an ACK within T seconds, he assumes the attempt has failed. The parameter is known to the clients as well as the server[4][5].

It is better to partition time to a sequence of windows, W1,W2,W3……,each of duration T . I suppose that the server can process requests at a mean rate of S REQ packets per second so that, in any window, the mean number of requests that it can process is ST . In any given window W, new clients arrive at a rate of $R(W)= \rho(W)S$ clients per second. The client request factor $\rho(W)=R(W)/S$ determines the fraction of the server's (computational) bandwidth that is required to process new clients in the window W . I assume that the client request factors are uniformly bounded above by $0\leq\rho(W)\leq\rho_{max}\leq1$, for some fixed ρ_{max} in the unit interval.

I also assume that a diffuse, distributed, denial-of-service attack A in the server takes the form of a potential time varying flood of spurious REQ packets aimed at overcoming the server's capacity to process new REQs. I suppose that in any given window W, the attacker A sends spurious REQs at a rate of $A(W)= \alpha(W)S$ packets per second. The attack factor $\alpha(W)=A(W)/S$ determine the extra bandwidth that will be required of the server to process the illegal requests in window W. Assume that the attack factors are uniformly bounded,$0\leq\alpha(W)<\alpha_{max}$, for some fixed ,though the upper bound on the attack factors may be very large. Clearly, when $\alpha(W)>1$, the attack overwhelms the server's capacity to process all requests unless there is a mechanism to efficiently handle the attack packets. My interest is in the case where $\alpha_{max}>>1$ and the attack can be occur on a scale much larger than the available server bandwidth[4][9].

In order to focus the DoS attack at the receiver, I listened the situation and assume that REQ and ACK packets are transmitted instantaneously , the round-trip delay obtained solely by processing time at the server, and that no REQ or ACK packets are lost in the time of transmission. Packet drops at the server are then obtained only because the arriving requests from clients and attackers combined and exceeds the server's computational bandwidth. Thus, if $\rho_{max}+\alpha_{max}>1$, then it cannot be guaranteed that a client's REQ will be processed by the server. If $\alpha_{max}>>1$, it is in principle then possible to almost completely compel the clients of service and results a successful DoS attack[7][8].

A.Request Rate,Bandwidth ,Time Enhancement

Here the Client Side protocol is same as that of ASV protocol . In the Server Side , I Introduced a small rule-Request rate,Band Width,TimeLimit(RBT)rule based on the ASV protocol. The Adaptive Selective Verification (ASV) protocol is a cost-based, DoS-resistant-protocol in which bandwidth is the currency. ASV protocol imagines the shared channel model as its fundamental attack model. That is the key idea of the protocol is for clients to spend more bandwidth with attacker's bandwidth usage, and the server to selectively process incoming requests. If a client attempts to acquire the current level of attack by replicating exponentially its requests up to a threshold, then the severity of attack increases. So the server implements a RBT sampling algorithm to collect a random

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

sample of the incoming packet requests and process them at its mean processing rate[4][5][9].

B .Requst Rate,Bandwidth,TimeLimit Enhancement of The Clients

The client first understands the attack rate , then adaptively increases the number of Request that sends in succeeding time out window.

1.Start with sending one req.
2.Double count of the Request: Send 2^x Request packets to the server.
3. Check for Time out: If no ACK packet is received within time T seconds, set x to x+1; if an ACK packet is received, exit the protocol and proceed to the next phase of communication.

C. Requst Rate,Bandwidth,TimeLimit Enhancement of The SERVER[5]

Find the Server Capacity S,Given request factor rrf and attack factor af;0<rrf<1,0<af<1

1.Initialize the window count zero to max.
2.[Form the reservoir]Store the arriving packets in to the reservoir.
3.Apply RBT Rule to the sampling packets
a)SET UP reqrrt
b)SET UP TMax
c)Find out fband
i)Calculate av THEN bl=av
ii)Find out atrng=totalbw/cnt
iii)IF atrng>bl
THEN
fband=avgw/2
ELSE
fband=bl
d) IF(t>tmax)||(req>reqrrt)||(us>fband)
THEN block clients ,RTB buffer stores actual requests
ELSE
Send ack.
4.Empty the reservoir and go to step1

VI.PROPOSED SYSTEM ADVANTAGES:

- In proposed system, we use bandwidth set by client's timeout window and change dynamically, and threshold value setup to block attacks.
- Congestion will not formulate here.
- We can evaluate attack parameters that known by clients and servers for security. We also understand the performance analysis of various attackers. Monitor client server process with RBT enhancement. Get every request properties from client.
- Deflect the attackers, and make separate blog for their properties. Block access to server.
- Clients delay can be minimized in process.
- Server side utilization is high.

VII.CONCLUSION

The proposed system RTB Enhancement on server side based on ASV uses a protocol which is highly adaptive to the arriving attack rates. This scheme uses bandwidth as currency. The level of protection employed by the clients is that they dynamically adjust to the current level of attack rates. At a high level of the attack, the clients ramp-up exponentially the number of requests they send in consecutive time windows, up to a maximum which is maintained at the client. In this System, the server implements a small process called RequestRate-Time-Bandwidth enhancement based on Adaptive Selective Verification protocol instead of random sampling to effectively sample from a sequence of incoming packets using bounded space. From my work, calculating attack rate and request rate to form a rule to attackers, and succeed for that. No system doesn't allow attackers through network to access server. But I can find a problem over there, that our system calculating attack rate by timeout window in the base. Another cause there may be a network failure or some other problem may be there through packet transferring. So that, I am planning to enhance my system by applying some more log properties of clients for finding attack rate through clients. So that it can avoid the clients block as attackers through network.

ACKNOWLEDGEMENT

The author would like to thank **Mr.S.Ramkumar** for the his inputs and support for this work. Thanks to the authors **Sanjeev Khanna**, **Santosh S. Venkatesh**, Member, IEEE and **Aziz Baayer**, **Nourddine Enneya**, **Mohammed Elkoutbi** Laboratory SI2M, ENSIAS, University of Mohammed-V-Souissi, Rabat, Morocco, Laboratory LaRIT, Faculty of Sciences, University of Ibn Tofail, Kenitra, Morocco for existing paper.

REFERENCES

[1] Sachin Lalar "Security in MANET: Vulnerabilities, Attacks & Solutions", International Journal of Multidisciplinary and Current Research, Vol.2 (Jan/Feb 2014)
[2] Aziz Baayer, Nourddine Enneya, Mohammed Elkoutbi, "Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs", Journal of Information Security, vol 3, 224-230,2012.
[3] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
[4] Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM- "Adaptive Selective Verification:An Efficient Adaptive Countermeasure to Thwart DoS Attacks",*IEEE/ACM TRANSACTIONS ON NETWORKING*, VOL. 20, NO. 3, JUNE 2012
[5] M.Padmadas ,Dr.N.Krishnan, Sreeja Nair M.P, "RTB Rule Based Adaptive Selective Verification Protocol To Prevent DoS Attack", *IEEE,International Conference on Computational Intelligence and Computing Research,Dec 2013.*
[6] ZHANG FU- "Multifaceted Defence Against Distributed Denial of Service Attacks: Prevention Detection", Mitigation, Division of Networks and Systems Department of Computer Science and Engineering CHALMERS UNIVERSITY OF TECHNOLOGY Gothenburg, Sweden 2012.
[7] M. Abadi, M. Burrows, M. Manasse, and T.Wobber, "Moderately hard,memory-b functions," Trans. *Internet Technol., vol. 5, no. 2, pp. 299–327, 2005.*
[8] C. A. Gunter, S. Khanna, K. Tan, and S. S. Venkatesh, "DoS protection for reliably authenticated broadcast," presented at *the NDSS, 2004*
[9] M. Arshey, C.Balakrishnan, "Adaptive defense strategy: immunizing shared channel network from dos attacks".*International Journal of Emerging Technology and Advanced Engineering , vol. 3, no. 1, pp. 209,2013.*

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

[10] www.icacci-conference.org
[11] SonicWALL, Inc.1160 Bordeaux Drive Sunnyvale, CA94089-12091-888-557-6642 http://www.sonicwall.com
[12] M. AlTurki, J. Meseguer, and C. A. Gunter, "Probabilistic modelling and analysis of DoS protection for the ASV protocol," *Electron. Notes Theoret. Comput. Sci., vol. 234, pp. 3–18, 2009*.
[13] Raj Kamal,Mobile Computing,"*Oxford University Press 2007*".

BIOGRAPHY

Sreeja Nair M P, a faculty member of computer science and Engineering in Cochin University College of Engineering kuttanad ,Alappuzha,kerala under Cochin Univesity of Science And Technology. During the initial phase of her career, she worked as a lecturer in College of Engineering ,Adoor, Pathanamthitta, Kerala(2008-2012).She did her MTech in Computer And Information Technology with specialisation Computer Communication.She has a paper on "RTB Rule Based on Adaptive Selective Verification Protocol To Prevent Dos Attack".It was presented on International Conference on Computational Intelligence and Computing Research,Dec 2013. She is doing her phd work self and will register soon. Her area of interest include Network Security in Computer Networks and Mobile Networks.Also she is interested on cloud computing,Grid Computing And Digital Image Processing.